



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003309558 A**

(43) Date of publication of application: **31.10.03**

(51) Int. Cl. **H04L 9/32**
G06F 15/00
G09C 1/00
H04L 9/08
H04L 12/28
H04Q 7/38

(21) Application number: **2003028278**

(22) Date of filing: **03.02.03**

(30) Priority: **08.02.02 US 2002 088699**

(71) Applicant: **XEROX CORP**

(72) Inventor: **BALFANZ DIRK**
LOPES CRISTINA V
SMETTERS DIANA K
STEWART PAUL JOSEPH
WONG HAO-CHI

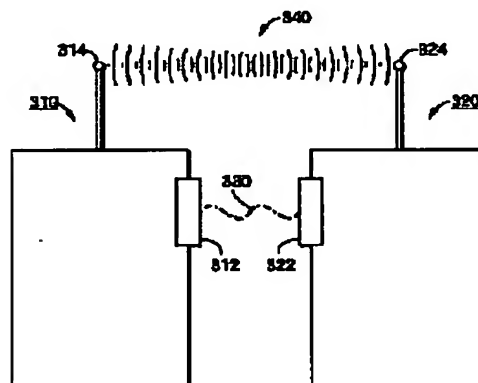
**(54) METHOD FOR AUTHENTICATING
COMMUNICATION ON NETWORK MEDIUM**

(57) Abstract

PROBLEM TO BE SOLVED: To guarantee the communication among a plurality of devices.

SOLUTION: This method for guaranteeing the communication between at least two devices on a network medium includes a step of transmitting previous authentication information from a first radio device 310 to a second radio device 320 on a position-limited channel, and a step of using the previous authentication information guaranteed by a second radio device 320 so as to authenticate the communication from the first radio device 310.

COPYRIGHT: (C)2004,JPO



(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-309558
(P2003-309558A)

(43) 公開日 平成15年10月31日 (2003.10.31)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/32		G 0 6 F 15/00	3 3 0 C 5 B 0 8 5
G 0 6 F 15/00	3 3 0	G 0 9 C 1/00	6 4 0 E 5 J 1 0 4
G 0 9 C 1/00	6 4 0	H 0 4 L 12/28	3 0 0 Z 5 K 0 3 3
H 0 4 L 9/08		9/00	6 7 5 B 5 K 0 6 7
12/28	3 0 0	H 0 4 B 7/26	1 0 9 R
審査請求 未請求 請求項の数8 O L (全 12 頁) 最終頁に続く			

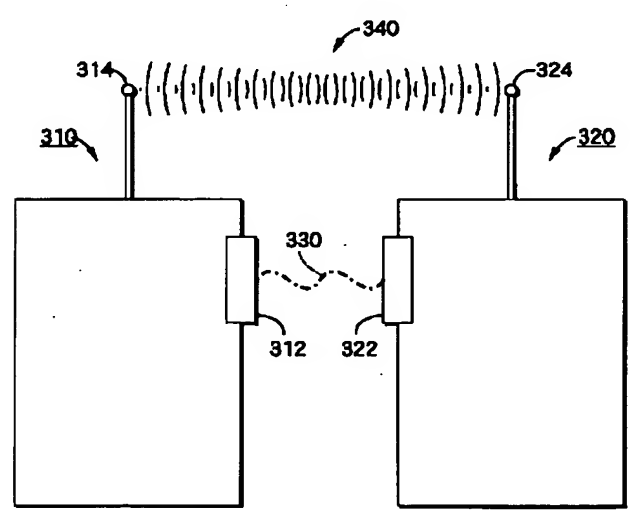
(21) 出願番号 特願2003-26278(P2003-26278)
(22) 出願日 平成15年2月3日 (2003.2.3)
(31) 優先権主張番号 10/066, 699
(32) 優先日 平成14年2月6日 (2002.2.6)
(33) 優先権主張国 米国 (US)

(71) 出願人 590000798
ゼロックス・コーポレーション
アメリカ合衆国、コネチカット州、スタン
フォード、ロング・リッジ・ロード 800
(72) 発明者 ダーク パルファンツ
アメリカ合衆国 カリフォルニア メンロ
パーク シャロン パーク ドライブ
600 アパートメント ディー103
(74) 代理人 100075258
弁理士 吉田 研二 (外1名)

最終頁に続く

(54) 【発明の名称】 ネットワーク媒体上で通信を認証するための方法

(57) 【要約】
【課題】 複数のデバイス間の通信を保障する。
【解決手段】 ネットワーク媒体上における少なくとも2つのデバイス間での通信を保障する方法であって、位置限定チャネル上で第1の無線デバイス310から第2の無線デバイス320に事前認証情報を送信するステップと、第1の無線デバイス310からの通信を認証するため第2の無線デバイス320によって保障された事前認証情報を使用するステップとを含む方法。



【特許請求の範囲】

【請求項1】 ネットワーク媒体上における少なくとも2つのデバイス間での通信を保障する方法であって、位置限定チャンネル上で第1のデバイスから第2のデバイスに事前認証情報を送信するステップと、前記第1のデバイスからの通信を認証するため前記第2のデバイスによって保障された前記事前認証情報を使用するステップと、を含むことを特徴とする方法。

【請求項2】 請求項1に記載の方法であって、位置限定チャンネル上で前記事前認証情報を送信するステップが、少なくとも、第1のシークレットへのコミットメントおよび意味があるメッセージへのコミットメントを含むコミットメントを前記第1のデバイスから前記第2のデバイスに送るステップと、少なくとも、第2のシークレットへのコミットメントおよび前記第2のデバイスから前記第1のデバイスへの意味がないメッセージへのコミットメントを含むコミットメントを送信することにより、前記第1のデバイスからのコミットメントに応答するステップと、前記第1のデバイスによって前記第2のデバイスのコミットメントの受信を承認するステップと、前記第2のデバイスによって前記第1のデバイスのコミットメントの受信を承認するステップと、を含むことを特徴とする方法。

【請求項3】 ネットワーク媒体上におけるデバイスのグループ間での通信を保障する方法であって、グループの少なくとも1つのデバイスをグループマネージャとして指定するステップと、放送位置限定チャンネルを使用して前記グループマネージャとグループの他のデバイスとの間の事前認証情報を交換するステップと、前記交換された事前認証情報であって、ネットワーク媒体上で通信を認証するために前記グループマネージャと前記グループの他のデバイスとによって保障された事前認証情報を使用するステップと、を含むことを特徴とする方法。

【請求項4】 請求項3に記載の方法であって、さらに、前記グループマネージャから前記グループ中の他のデバイスにグループキー情報を分配するためにネットワーク媒体を使用するステップを含むことを特徴とする方法。

【請求項5】 請求項3に記載の方法であって、さらに、デバイスの前記グループ中に新しいデバイスを受信するステップと、前記放送位置限定チャンネルを使用して前記グループマネージャと前記新しいデバイスとの間で事前認証情報を交換するステップと、

前記交換された事前認証情報であって、ネットワーク媒体上で通信を認証するために前記グループマネージャと前記新しいデバイスとによって保障された事前認証情報を使用するステップと、を含むことを特徴とする方法。

【請求項6】 請求項3に記載の方法であって、デバイスがデバイスの前記グループを離れる場合、さらに、前記グループの他の残っているデバイスに対して前記グループマネージャの事前認証情報を無効にするステップと、前記グループマネージャによって前記グループ中の残っているデバイスに新しい事前認証情報を分配するステップと、前記グループマネージャと前記グループ中の残っているデバイスとによって分配された事前認証情報であって、前記グループマネージャと前記グループ中の残っているデバイスとの間での通信を認証する事前認証情報を使用するステップと、を含むことを特徴とする方法。

【請求項7】 請求項6に記載の方法であって、さらに、前記グループマネージャから前記グループ中の残っているデバイスに新しいグループキー情報を分配するためにネットワーク媒体を使用するステップを含むことを特徴とする方法。

【請求項8】 ネットワーク媒体上におけるデバイスのグループ間での通信を認証する方法であって、放送位置限定チャンネル上で各デバイスとグループ中の他のデバイスとの間で事前認証情報を交換するステップと、ネットワーク媒体上で選択されたデバイスとの通信を認証し通信しているデバイスによって保障された通信のために選択されたデバイスの事前認証情報を使用するステップと、を含むことを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク媒体を使用して送信される少なくとも2つのデバイス間の通信を認証するためのシステムおよび方法に関する。

【0002】

【従来の技術】ネットワーク通信によりユーザはネットワーク媒体上で文書などの情報を受信できるようになった。ネットワーク媒体は有線ネットワークおよび無線ネットワークを含む。ネットワーク媒体上で送信される情報は他者にとってアクセス可能である。しかしながら、ユーザは一般に受信されるそのような情報が他者にとって利用可能でないことを望む。

【0003】

【発明が解決しようとする課題】本発明は、複数のデバイス間の通信を保障することを目的とする。

【0004】

【課題を解決するための手段】本発明によれば、いくつかの無線デバイスを事前認証することを使用して、任意のピアツーピアアドホック (peer-to-peer ad-hoc) 対話を確実に認証する。ここでは、暗号化チャンネルをセットアップするために使用されるキー交換プロトコルへのブートストラップ (bootstrap) を含んでもよい。パブリックキーが事前認証チャンネル上でコミットされる。パブリックキー暗号法を使用するキー交換プロトコルを主無線リンク中で使用して確実な通信を確立する。パブリックキーを使用して無線デバイスを事前認証するため、位置限定チャンネル (location limited channel) として使用可能な媒体のタイプは盗聴を心配する必要がなく、例えば可聴周波および/または赤外チャンネルを含むことができる。パブリックキーを使用して無線デバイスを事前認証することにより、無線デバイスを認証することができる一連のパブリックキーベースキー交換プロトコルが使用できるようになる。

【0005】

【発明の実施の形態】図1は無線システム300の1つの例示的な実施形態を示す。2つだけの無線デバイス310および320が示されている。しかしながら、システム300は3つ以上の無線デバイスを含むことができる。第1の無線デバイス310は位置限定チャンネル受信機/送信機312および主無線リンク受信機/送信機314を含む。同様に、第2の無線デバイス320は位置限定チャンネル受信機/送信機322および主無線リンク受信機/送信機324を含む。代替実施形態では、第1および第2の無線デバイスはそれぞれトランスポートコントロールプロトコル/インターネットプロトコル (TCP/IP) ソケットや他の知られているかまたは後で開発された有線ネットワーク受信機/送信機などの主無線リンク受信機/送信機を有する。別の実施形態では、第1および第2の無線デバイスはどちらも主無線リンクおよび主有線リンクを有する。

【0006】第1の無線デバイス310が第2の無線デバイス320との通信を開始した場合、第1の無線デバイス310は最初に事前認証情報を位置限定チャンネル330を介して位置限定チャンネル受信機/送信機312を通して第2の無線デバイス320に送る。第2の無線デバイス320は事前認証情報を第1の無線デバイス310から位置限定チャンネル受信機/送信機322を通して受信する。

【0007】相互認証が不要な場合、第1の無線デバイス310は第2の無線デバイス320に事前認証情報を送る必要はない。別の無線デバイスと事前認証情報を相互に交換しない無線デバイスは他の無線デバイスから受信した通信を認証することができない。したがって、その無線デバイスは盗聴者による攻撃から保護されない。

したがって、2つの無線デバイス間での機密情報の交換など、相互認証が必要な場合、第2の無線デバイス320は追加の事前認証情報を位置限定チャンネル330を介して位置限定チャンネル受信機/送信機322を通して無線デバイス310に送ることによって応答する。

【0008】第1の無線デバイス310はその位置限定チャンネル受信機/送信機312を通して事前認証情報を受信する。事前認証情報が第1の無線デバイス310と第2の無線デバイス320の間で交換されると、第1の無線デバイス310は主無線リンク受信機/送信機314を使用して主無線リンク340を介して第2の無線デバイス320と通信する。第2の無線デバイス320はその主無線リンク受信機/送信機324を使用して主無線リンク340を介して第1の無線デバイス310と通信する。事前認証情報が2つの無線デバイス310および320間で両方向に交換されているので、第1および第2の無線デバイス310および320の各々は、それぞれ他方の無線デバイス320または310から受信した受信事前認証情報を使用して、それぞれその他方の無線デバイス320または310の通信を認証する。

【0009】図2は無線デバイス400の1つの例示的な実施形態を示す。無線デバイス400はパーソナルデジタルアシスタント (PDA)、無線能力をもつラップトップコンピュータ、無線ハンドヘルドコンピュータ、Blackberry (R) デバイス、無線能力をもつプリンタ、無線フォンなどとして使用することができる。無線デバイス400は、プロセッサ410、メモリ420、入出力 (I/O) インターフェース430、位置限定チャンネル受信機/送信機442および主無線リンク受信機/送信機444を含む。

【0010】メモリ420はオペレーティングシステム422、無線アプリケーション424、認証アプリケーション426および認証器428の各プログラムを記憶する。オペレーティングシステム422はプロセッサ410によって実行されると無線デバイス400の入出力インターフェース430を含む様々な入出力コントローラをプログラムし、制御する。オペレーティングシステム422は無線アプリケーション424、認証アプリケーション426および認証器428を検索可能な状態で記憶する命令を提供する。

【0011】無線アプリケーション424は無線デバイス400が入出力インターフェース430の主無線リンクインターフェース434に接続された主無線リンク受信機/送信機444を通して無線ネットワークと通信できるようにする命令を提供する。無線アプリケーション424はBluetooth (R)、ANSI/IEEE 802.11などとして使用することができる。

【0012】無線ネットワーク中で使用される無線受信機/送信機は主無線リンクインターフェース434および主無線リンク受信機/送信機444として使用するこ

とができる。代替実施形態では、無線デバイスはTCP/IPインターフェースおよびソケットなどの主有線リンクインターフェースおよび主無線リンク受信機/送信機または主無線リンクインターフェースおよび送信機ならびに主有線インターフェースおよび受信機/送信機を有する。

【0013】位置限定チャンネル受信機/送信機442は主無線リンク受信機/送信機444とは別にすることができる。適切な位置限定チャンネル受信機/送信機442は無線デバイスの事前認証情報を送受信するために少なくとも2つのプロパティを有する。第1のそのようなプロパティは例証的(demonstrative)プロパティである。適切な位置限定チャンネル受信機/送信機442はその送信における物理的制限を有する。例えば、送信範囲および放送特性が制限されている、可聴周波範囲内および/または超音波範囲内の音声は無線デバイスのグループ用の位置限定チャンネルとして使用されることがある。2つの無線デバイス間などポイントツーポイント通信では、赤外チャンネルなど方向性をもつ位置限定チャンネルが使用されることがある。例証的プロパティによればデバイスと位置限定チャンネルを通してアクセス可能な限定された位置との間の物理的関係に基づいてターゲットデバイスまたはデバイスのグループを「名付ける」ために位置限定チャンネル上で通信を行うことが可能になる。

【0014】第2のプロパティは信頼性(authenticity)である。このプロパティによれば、盗聴が存在する場合でも、位置限定チャンネル上で交換される事前認証情報により交換している無線デバイスが主無線リンク上で互いを確実に認証することができる。関係者が位置限定チャンネルを使用してそれらのパブリックキーを事前認証情報として交換する場合、盗聴者は関係者のプライベートキーを知らないので位置限定チャンネル上での盗聴者による攻撃は重要ではない。関係者はキー交換プロトコルの一部としてそれらの対応するプライベートキーの保有を証明することによって主無線リンク上で互いを認証することになる。したがって、盗聴者はいずれの関係者をも装うことができない。

【0015】位置限定チャンネル受信機/送信機の別のプロパティは、攻撃が少なくとも1つの合法参加者(人間またはデバイス)によって検出されることなしに位置限定チャンネルを攻撃することが困難なことである。これらは赤外、可聴周波および/または超音波の音声、および/または本体上での近接場信号を使用する受信機/送信機を含む。

【0016】攻撃を検出する場合、位置限定チャンネル上で送信しているデバイスが特定される必要はないことがある。代わりに、例えば、攻撃を検出することは単に人の計数する能力に依存することがある。したがって、2つの無線デバイスが通信しようと試み、例えばターゲッ

トデバイス上の光が明滅することによって、またはラップトップコンピュータを使用している人間が通信が成功したことを示すことによって、通信が成功したことが示された場合、合法関係者の数が知れる。例えば、第3の関係者が通信に参加していることをラップトップが示すことによって、余分な違法の関係者が検出された場合、通信は単に合法関係者によって中止されることがある。

【0017】事前認証情報は受信した認証器428を認証するために使用される。認証器428はキー、シークレットなどとして使用することができる。キーは長命キーかまたは短命キーとして使用することができる。選択は通常キーが使用されているアプリケーションに基づく。いずれの場合にも、キーは信用されている権威による証明を必要としない。しかしながら、選択されるキー交換プロトコルが証明書交換を必要とする場合、証明書は無線デバイス400によって自己署名される。

【0018】通常、位置限定チャンネル上で交換される情報の量は主無線リンク上で送られる情報の量の小部分である。事前認証情報のサイズを縮小する1つの方法は、例えばSecure Hash Algorithm-1(SHA-1)などの暗号法上安全なハッシュ関数を使用することである。この方法を使用すると、関係者は実際にそれらの完全なパブリックキーを事前認証情報として交換する必要がない。代わりに、関係者は、例えばキーのダイジェストを交換することによってキーのコミットメントを送る。関係者は選択された位置限定チャンネル上でそれらのパブリックキーへのコミットメントを交換する。そうすることで、各関係者は、その関係者が通信している人を特定することができる。

【0019】無線デバイス400は主無線リンク受信機/送信機444を使用して別の無線デバイスと通信する。無線デバイス400は、市販されているSecure Socket Layer/Transport Layer Security(SSL/TLS)、Secure Key Exchange Mechanism(SKEME)、Internet Key Exchange(IKE)などの様々な確立されたパブリックキーベースキー交換プロトコルを含む認証アプリケーション426を使用して、事前認証情報交換中にコミットされたパブリックキーに対応するプライベートキーの保有を証明する。その場合、パブリックキーのダイジェストが事前認証情報交換中に送られた場合、無線デバイス400は主無線リンク上で完全なパブリックキーを交換する。キー交換はプロトコル実行にプレフィクスされるか、またはSocket Layer/Transport Layer Security(SSL/TLS)の場合のように、キー交換プロトコルの標準部分として当然行われる。キーはそれらが位置限定チャンネル上でコミットされたものであったという事実によって認証される。他の無線デバイスのパブリックキーを認証

した無線デバイス400は主無線リンク上で交換プロトコルを続行する。

【0020】図3はネットワーク媒体上で通信を認証する1つの方法を概説するフローチャートである。ステップS100から始めて、オペレーションはステップS110に進み、そこで第1の無線デバイスは第2の無線デバイスに位置限定チャンネルを使用してパブリックキーPK₁へのコミットメントを送る。これは位置限定チャンネル上での事前認証情報の交換の少なくとも一部である。コミットメントはパブリックキー自体、証明書、またはパブリックキーのダイジェストとすることができる。ステップS120で、第1の無線デバイスからパブリックキーPK₁へのコミットメントを受信したことに応答して、第2の無線デバイスは第1の無線デバイスによって受信される位置限定チャンネル上でパブリックキーPK₂へのコミットメントを送る。この段階で、第1の無線デバイスは主無線リンク上での通信に備えるために第2の無線デバイスのアドレスを受信することもできる。

【0021】ステップS130で、第1の無線デバイスは主無線リンクを使用して第2の無線デバイスにパブリックキーPK₁を送る。ステップS140で、第2の無線デバイスはそのパブリックキーPK₂を第1の無線デバイスに送り、キーの交換が行われる。ステップS150で、第1の無線デバイスは第2の無線デバイスから受信したパブリックキーPK₂を認証し、パブリックキーPK₂を事前認証情報段階で受信したコミットメントと比較する。一実施形態では、受信したパブリックキーPK₂の認証は、パブリックキーに対応するプライベートキーの所有権を証明する図2に示されるものなどのキー交換プロトコルを使用して実施される。第1の無線デバイスがそのパブリックキーPK₁を主無線リンク上で送るときに第2の無線デバイスがシークレットS₂を使用している場合、第2の無線デバイスはパブリックキーPK₁をコミットメントに対して検証し、それを使用してそのシークレットS₂を暗号化し、結果EPK₁(S₂)を第1の無線デバイスに戻す。認証はシークレットS₂を生成する第2の無線デバイスの能力および結果EPK₁(S₂)を復号する第1の無線デバイスの能力によって実施される。

【0022】ステップS160で、前に第2の無線デバイスから受信したパブリックキーPK₂のコミットメントが受信したパブリックキーPK₂に一致するかどうかの決定がなされる。そうである場合、オペレーションはステップS170に進む。それ以外の場合、オペレーションはステップS180に飛ぶ。S170において第1の無線デバイスは、通信を暗号化するためにキー交換プロトコル中に同意された対称キーを使用して主無線リンク上で第2の無線デバイスとの通信を再開する。次いでオペレーションはS190に飛ぶ。反対に、ステップS180で、第1の無線デバイスが第2の無線デバイスの

パブリックキーPK₂を認証することができない場合、第1の無線デバイスは第2の無線デバイスとの通信を終了する。次いでオペレーションはステップS190に進み、そこで方法は終わる。

【0023】様々な例示的な実施形態では、第1の無線デバイスは乱数などの任意のシークレットS₁を含むことを理解されたい。この場合、第1の無線デバイスは任意のシークレットS₁へのコミットメントを送っているため、S₁はシークレットのままであるべきなのでコミットメントは暗号法ダイジェストh(S₁)の形態で送られる。様々な他の例示的な実施形態では、第1の無線デバイスは、主無線リンクでの通信に備えるためにIPアドレスおよびポート番号、Bluetoothデバイスアドレス、ユーザフレンドリ名または他の適切な情報など、そのアドレスを送信することもできる。

【0024】図4～図6は、対話通信に備える改善されたGuy Fawkesプロトコルを実施する方法の1つの例示的な実施形態を概説するフローチャートである。この方法は、パブリックキーオペレーションが実行不可能であるような無線デバイスの計算リソースが制限されており、位置限定チャンネルがシークレットデータの信用されている交換を提供しない場合に使用することができる。

【0025】図4～図6に示すように、オペレーションはステップS200で始まり、ステップS205に進み、そこでカウンタNは1にセットされる。ステップS210で、第1の無線デバイスは、第2の無線デバイスに位置限定チャンネル上でそのN番目のメッセージのダイジェストとともにそのN番目のメッセージを認証するために使用されることになるそのN番目のシークレット(認証器)のダイジェストを含むN番目の通信を送る。ステップS215で、第2の無線デバイスは、第1の無線デバイスに位置限定チャンネル上でそのN番目のメッセージのダイジェストとともにそのN番目のメッセージを認証するために使用されることになるそのN番目のシークレットのダイジェストを含むN番目の通信を送る。

【0026】ステップS220で、第1の無線デバイスは第2の無線デバイスに第2の無線デバイスのN番目の通信のダイジェストおよび第1の無線デバイスのN番目のシークレットを送る。ステップS225で、第2の無線デバイスは第1の無線デバイスに第1の無線デバイスのN番目の通信のダイジェストおよび第2の無線デバイスのN番目のシークレットを送る。ステップS230で、第1および第2の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第1の無線デバイスまたは第2の無線デバイスが通信を終了すると決定した場合、オペレーションはステップS320に進む。その他の場合、通信は継続し、オペレーションはステップS235に進む。

【0027】ステップS235で、第1の無線デバイスは主無線リンク上で通信を継続する。通信の開始者として、第1の無線デバイスは、第2の無線デバイスに、意味があるN番目のメッセージと、(N+1)番目のメッセージのダイジェストを含む(N+1)番目の通信とともにその(N+1)番目のメッセージを認証するために使用されることになるその(N+1)番目のシークレットのダイジェストとを送る。ステップS240で、第2の無線デバイスは、第1の無線デバイスに、意味がないN番目のメッセージと、(N+1)番目のメッセージのダイジェストを含む(N+1)番目の通信とともにその(N+1)番目のメッセージを認証するために使用されることになるその(N+1)番目のシークレットのダイジェストとを送る。第2の無線デバイスのN番目のメッセージは、第2の無線デバイスがステップS210で送信された第1の無線デバイスのN番目のメッセージを知らないときにステップS215でコミットされたものなので意味がない。この時点で、無線デバイスのいずれかが通信を終了することができる。したがって、ステップS245で、第1および第2の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第1の無線デバイスまたは第2の無線デバイスが通信を終了すると決定した場合、オペレーションはステップS320に進む。その他の場合、通信は継続し、オペレーションはステップS250に進む。

【0028】ステップS250で、第1の無線デバイスは第2の無線デバイスに第2の無線デバイスの(N+1)番目の通信のダイジェストおよび第1の無線デバイスの(N+1)番目のシークレットを送る。ステップS255で、第2の無線デバイスは第1の無線デバイスに第1の無線デバイスの(N+1)番目の通信のダイジェストおよび第2の無線デバイスの(N+1)番目のシークレットを送る。

【0029】ステップS260で、第1の無線デバイスは、第2の無線デバイスに、意味がない(N+1)番目のメッセージと、(N+2)番目のメッセージのダイジェストを含む(N+2)番目の通信とともにその(N+2)番目のメッセージを認証するために使用されることになるその(N+2)番目のシークレットのダイジェストとを送る。第1の無線デバイスの(N+1)番目のメッセージは、意味があるメッセージを送る順番が第2の無線デバイスなので意味がない。ステップS265で、第2の無線デバイスは、第1の無線デバイスに、意味がある(N+1)番目のメッセージと、(N+2)番目のメッセージのダイジェストを含む(N+2)番目の通信とともにその(N+2)番目のメッセージを認証するために使用されることになるその(N+2)番目のシークレットのダイジェストとを送る。第2の無線デバイスは、第2の無線デバイスが意味がある第1の無線デバイスのN番目のメッセージを知った後でステップS

240でコミットメントがなされたために意味があるメッセージを送る。ステップS270で、第1および第2の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第1の無線デバイスまたは第2の無線デバイスが通信を終了すると決定した場合、オペレーションはステップS320に進む。その他の場合、通信は継続し、オペレーションはステップS275に進む。

【0030】ステップS275で、第1の無線デバイスは第2の無線デバイスに第2の無線デバイスの(N+2)番目の通信のダイジェストおよび第1の無線デバイスの(N+2)番目のシークレットを送る。次に、ステップS280で、第2の無線デバイスは第1の無線デバイスに第1の無線デバイスの(N+2)番目の通信のダイジェストおよび第2の無線デバイスの(N+2)番目のシークレットを送る。ステップS285で、第1の無線デバイスは、第2の無線デバイスに、意味がない(N+2)番目のメッセージと、(N+3)番目のメッセージのダイジェストを含む(N+3)番目の通信とともにその(N+3)番目のメッセージを認証するために使用されることになるその(N+3)番目のシークレットのダイジェストとを送る。(N+2)番目のメッセージは、第1の無線デバイスが意味がある第2の無線デバイスの(N+1)番目のメッセージを受信していないときに第1の無線デバイスがステップS260でコミットされたので意味がない。しかしながら、第1の無線デバイスは、第1の無線デバイスがステップS265で第2の無線デバイスからの意味がある(N+1)番目のメッセージを有していたので意味がある(N+3)番目のメッセージにコミットすることができる。

【0031】ステップS290で、第2の無線デバイスは、第1の無線デバイスに、意味がない(N+2)番目のメッセージと、(N+3)番目のメッセージのダイジェストを含む(N+3)番目の通信とともにその(N+3)番目のメッセージを認証するために使用されることになるその(N+3)番目のシークレットのダイジェストとを送る。第2の無線デバイスの(N+2)番目のメッセージは、「話す」次の順番が第1の無線デバイスに属するので意味がない。この場合も、この時点で、無線デバイスのいずれかが通信を終了することができる。したがって、ステップS295で、第1および第2の無線デバイスの一方または両方によって通信を終了すべきかどうかの決定がなされる。第1の無線デバイスまたは第2の無線デバイスが通信を終了すると決定した場合、オペレーションはステップS320に飛ぶ。その他の場合、通信は継続し、オペレーションはステップS300に進む。

【0032】ステップS300で、第1の無線デバイスは第2の無線デバイスに第2の無線デバイスの(N+3)番目の通信のダイジェストおよび第1の無線デバイ

スの(N+3)番目のシークレットを送る。ステップS305で、第2の無線デバイスは第1の無線デバイスに第1の無線デバイスの(N+3)番目の通信のダイジェストおよび第2の無線デバイスの(N+3)番目のシークレットを送る。ステップS310で、コントローラNは4に増分される。次いでオペレーションはステップS235に戻る。反対に、ステップS320で、方法のオペレーションは終わる。

【0033】相互認証が不要であるアプリケーションがあることを理解されたい。例えば、サービスを要求する誰かにサービスを提供するように設計されたデバイスは、それが通信しているデバイスを認証する必要はなく、したがって事前認証情報を送るべき唯一のデバイスとすることができる。そのようなデバイスは、例えば、無線空間中でその能動的プロキシを一意的にかつ確実に特定するのに十分な事前認証情報を送る赤外(IR)情報ビーコンまたは無線周波数特定(RFID)タグなどの受動的ビーコンを有することができる。そのような手法は、物理的目標に「デジタル存在」を提供するためにそのようなビーコンを使用するシステムにセキュリティおよび認証の尺度を追加するために使用することができる。

【0034】図2に関して説明した位置限定チャンネルの一部は放送能力を有する。そのような放送能力を使用すると、認証されたグループ通信に備えるプロトコルを構成することができる。アプリケーションにはネットワーク化されたゲームおよびミーティングサポートおよび/または会議ソフトウェアが含まれる。

【0035】可聴周波は放送位置限定チャンネルを提供することができる媒体である。可聴周波は関係者が監視し、追跡することができる。交換の関係者は、可聴周波メッセージ中に何が搬送されているかを知らない場合でも、そのような可聴周波メッセージを送っているべき合法グループ関係者を認識することができる。可聴周波は、関係者にフィードバックを提供するために多くのソフトウェアによってすでに使用されている音声に組み込むことができる。例えば、たいていの団体会議コールセッティングは新しい関係者がコールに入るときはいつでも短い「ジョイントーン」をならす。そのようなトーンは関係者のキー情報を含有するようにも変更することができる。すでに可聴周波および/または音声情報を搬送するように設計された指定されたチャンネルが存在するので、位置限定チャンネルとしての可聴周波を電話ネットワークを介して使用することができる。

【0036】位置限定チャンネル上でパブリックキー暗号法を使用することはそれらの交換が機密を必要とせず、したがって盗聴されにくいことを意味するので、可聴周波チャンネルの放送特性を使用してグループ通信を事前認証することができる。グループ通信の各関係者は、すべての他の合法関係者によって聞かれる可聴周波チャンネル

上でその関係者の事前認証情報を放送する。事前認証情報は概してパブリックキーへのコミットメントを含むことになる。放送はまた、攻撃者によって聞かれることがあるが、人間によってであろうとデバイスによってであろうと合法関係者によって検出されることなくそれらの攻撃者が可聴周波チャンネル上でそれら自体の事前認証情報を放送するようにしないかぎり、それによってプロトコルのセキュリティが危険にさらされることはない。位置限定チャンネル上で能動的攻撃を開始するためにそのように攻撃者の情報を放送しようと試みる攻撃者は通常、「余分な」放送があるので、合法人間またはデバイス関係者によって検出されることになる。例えば、可聴周波の場合、予期しない位置からの放送があることになる。

【0037】合法関係者は、図2に関して説明したものなど知られているかまたは後で開発されたグループキー交換プロトコルを続行し、各関係者は、位置限定チャンネル上で関係者によってコミットされたパブリックキーに対応するプライベートキーのその関係者の保有を1つまたは複数の合法関係者に証明する。そのようにコミットされたパブリックキーの1つに対応するパブリックキーの保有を証明することができる関係者はグループ通信中の認証される関係者と考えられる。さらに、選択されたキー交換プロトコルによりグループ通信の関係者間でさらなる通信を暗号化しかつ/または認証するために使用することができるいくつかの追加のキーをすべての関係者が共用することにもなる。

【0038】図7～図9はネットワーク媒体上で無線デバイスのグループ間で通信を認証するための例示的なセッティングを示す。図7に示すように、1つの関係者がグループマネージャ610として働く。事前認証情報を送るべき第1の関係者はグループマネージャ610になる。その他の場合、ランダムな関係者がグループマネージャ610として選択される。グループマネージャ610は、放送位置限定チャンネル上で様々な合法関係者612、614および616に事前認証段階中にグループパブリックキーへのコミットメントまたはそれ自身のパブリックキーなどの事前認証情報を放送する。図7に示すように、他の当事者622、624および626が存在し、無線ネットワークへのアクセス権を有する。位置限定チャンネル上で送信しようと試みると、合法関係者は通常位置限定チャンネル上のすべての送信を検出することができ、そのような送信の数を予想される送信の数、すなわち合法関係者の数と比較することができるので、その試みは検出されることになる。

【0039】図8に示すように、各関係者612、614および616はグループマネージャ610からの認証放送情報に応答して、位置限定チャンネル上でその関係者自身のパブリックキーへのコミットメントをそれぞれ含有するその関係者自身の事前認証情報をそれぞれ放送する。これらの放送はグループマネージャ610と他の合

10

20

30

40

50

法関係者612、614および616の両方によって受信される。その関係者の事前認証情報を放送した後、各関係者612、614および616は、例えば、グループマネージャの事前認証情報の一部としてグループマネージャ610によって提供されるアドレスを使用して、グループマネージャ610へのポイントツーポイント接続を行う。各関係者612、614および616はSocket Layer/Transport Layer Security (SSL/TLS)などのポイントツーポイントキー交換プロトコルでグループマネージャ610に10 関与する。そのプロトコルを使用して、グループマネージャ610は関係者612、614および616の各々に共用される1つまたは複数のグループ暗号キーのコピーを与える。これらのキーは、グループマネージャ610および他の関係者612、614および616を含むすべての関係者間でさらなる通信を暗号化し、認証するために使用される。

【0040】当事者622、624および626はそれらの事前認証情報を位置限定チャンネル上で放送しなかったため、グループマネージャ610はグループ通信中に合法関係者として当事者622、624および626を認識しない。したがって、当事者622、624および626はグループマネージャ610と主無線リンク上でポイントツーポイント接続をうまく生成することはできないことになる。この結果、当事者622、624および626はグループマネージャ610およびすべての他の当事者612、614および616を含む合法関係者間でグループ通信を復号することを可能にするであろう共用グループキーを受信しないことになる。

【0041】図10はネットワーク媒体上で無線デバイスのグループ間で通信を認証する方法の第1の例示的な実施形態を概説するフローチャートである。オペレーションはステップS400から始まり、ステップS410に進み、そこでグループの関係者のためのグループマネージャが選択される。ステップS420で、グループマネージャは位置限定チャンネル上でその事前認証情報をグループの関係者に放送する。一実施形態による事前認証情報はグループマネージャのパブリックキーのダイジェストとすることができる。ステップS430で、グループマネージャの事前認証情報を受信する各関係者はその事前認証情報をグループマネージャおよび他の関係者に送ることによってこたえる。グループマネージャを含む関係者間での事前認証情報の交換は、放送として、位置限定チャンネル上で行われる。一実施形態によれば、関係者の事前認証情報はその関係者のパブリックキーのダイジェストである。

【0042】ステップS440で、グループマネージャおよび関係者の各々は、例えば無線リンク上で知られているかまたは後で開発されたキー交換プロトコルを使用して、事前認証段階中に受信したパブリックキーのダイ

ジェストに対応するパブリックキーを使用してポイントツーポイントキー交換を実行する。そのようなプロトコルはまたグループマネージャとグループの現在関係者との間でポイントツーポイント暗号化および認証チャンネルをセットアップすることになる。ステップS450で、グループマネージャは共用セッションキーとして使用されるべきグループキーのコピーを無線リンク上で各関係者に分配することができる。ステップ460で、認証方法のオペレーションは終わり、グループマネージャを含むグループの関係者間で確実な通信を続行することが可能になる。

【0043】中央管理グループでは、関係者の加入および離脱を管理することは比較的容易である。加入する関係者はグループマネージャ610とともに上記で論じた2当事者プロトコルの1つを使用してそれ自体を認証し、保障された無線リンク上でグループキーを受信することができる。関係者がグループを離脱するとき、グループマネージャ610は無線リンク上ですべての残っている関係者に新しいグループキーを分配することができる。これはグループマネージャ610がポイントツーポイントキー交換中に各個別の関係者とともに共用シークレットキーを確立しているので行うことができる。

【0044】図11はネットワーク媒体上で無線デバイスのグループ間で通信を認証する別の方法を概説するフローチャートである。図11に概説する方法によればすべての関係者が等しくキー生成に関与することができ、したがって、すべての関係者が等しく信用することができる。

【0045】オペレーションはステップS500で始まり、ステップS510に進み、そこで各関係者は、放送位置限定チャンネルを使用してグループの関係者に、Diffie-Hellmanパブリック値へのコミットメントなど、その事前認証情報を放送する。ステップS520で、選択されたグループキー交換プロトコルを続行し、そこで関係者は無線ネットワーク上でそれらの完全なDiffie-Hellmanパブリック値を提示する。グループキー交換プロトコルは、すべての関係者がグループ共用シークレットキーの生成を分担することを可能にする、グループの関係者間の変更Diffie-Hellmanキー交換とすることができる。

【0046】標準の2当事者Diffie-Hellmanキー交換と同様に、シークレットが確立される間、グループの関係者は他人である。したがって、拡張Diffie-Hellmanに基づくこれらのプロトコルは、すべての関係者が共用パブリックキーインフラストラクチャに関与するか、または前に交換されたパブリックキーを有することを仮定する。

【0047】位置限定チャンネル上で交換された事前認証情報により関係者は互いに認証することができるので、この仮定はもはや不要である。放送位置限定チャンネルを

使用するとグループのすべての関係者はそれらのパブリックキーを公的にグループの1つまたは複数の関係者にコミットすることができる。ステップS530で、関係者は次いで無線リンク上で選択されたグループキー交換プロトコルを続行し、例えば、提示された完全なDiffie-Hellmanパブリック値を使用してグループキーを得る。オペレーションは次いでステップS540に進み、そこで認証方法のオペレーションは終わり、確実な通信を続行することが可能になる。

【0048】セッションが始まった後で加入した関係者は、その関係者が加入する際に位置限定チャンネル上でその関係者のキーコミットメントをグループの関係者の残りに放送することができる。ランダムに選択される現在関係者は応答して、相互認証を行うことができる。選択されたグループキー交換プロトコルは、これらの新しい関係者の共用グループキーを更新するか、または離脱する関係者のキーを無効にする詳細を扱うために使用される。

【図面の簡単な説明】

【図1】 本発明による通信認証システムを示す図である。

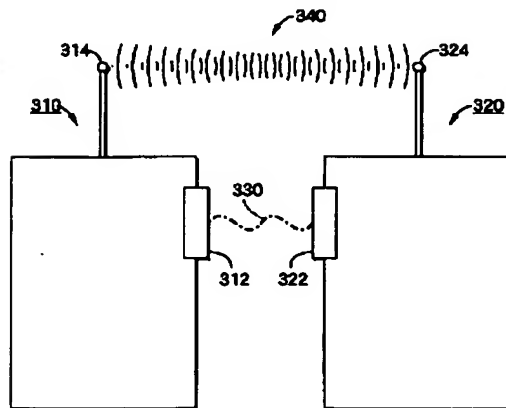
【図2】 本発明による無線デバイスを示す図である。

【図3】 本発明による通信を認証するための方法のフローチャートである。

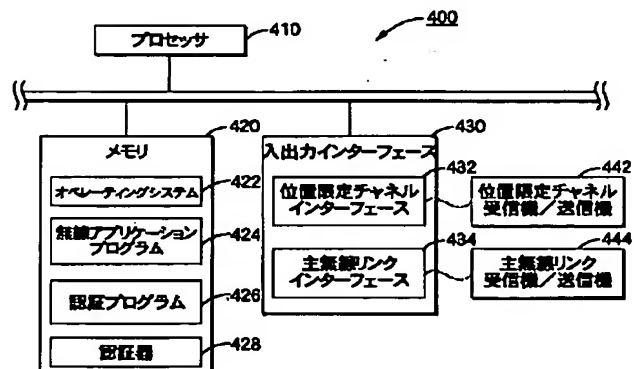
【図4】 本発明による通信を認証するための方法のフローチャートである。

【図5】 本発明による通信を認証するための方法のフ

【図1】



【図2】



ローチャートである。

【図6】 本発明による通信を認証するための方法のフローチャートである。

【図7】 本発明によるデバイスのグループの通信認証システムを示す図である。

【図8】 本発明によるデバイスのグループの通信認証システムを示す図である。

【図9】 本発明によるデバイスのグループの通信認証システムを示す図である。

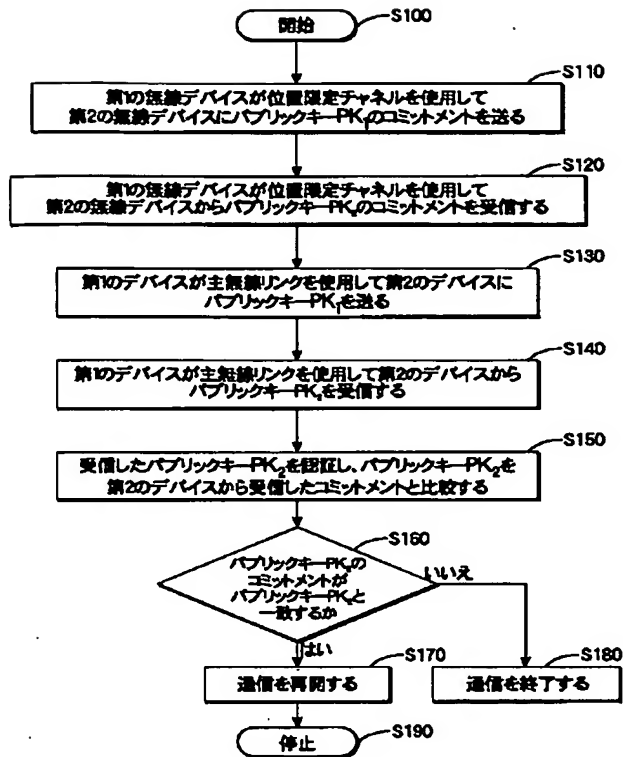
10 【図10】 本発明による通信を認証するための方法のフローチャートである。

【図11】 本発明による通信を認証するための方法の別のフローチャートである。

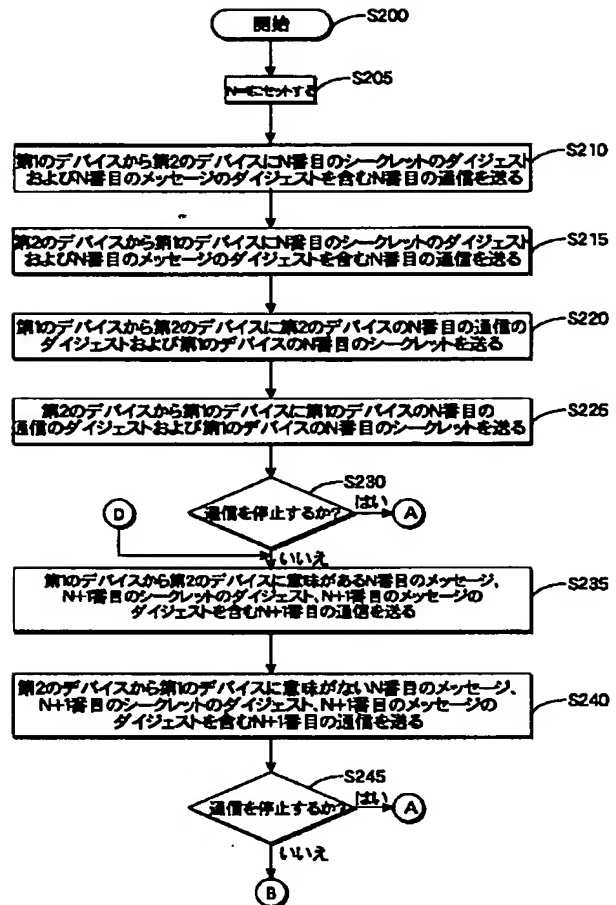
【符号の説明】

300 無線システム、310 第1の無線デバイス、312 位置限定チャンネル受信機/送信機、314 主無線リンク受信機/送信機、320 第2の無線デバイス、322 位置限定チャンネル受信機/送信機、324 主無線リンク受信機/送信機、330 位置限定チャンネル、400 無線デバイス、410 プロセッサ、420 メモリ、422 オペレーティングシステム、424 無線アプリケーションプログラム、426 認証プログラム、428 認証器、430 入出力インターフェース、432 位置限定チャンネルインターフェース、434 主無線リンクインターフェース、442 位置限定チャンネル受信機/送信機、444 主無線リンク受信機/送信機。

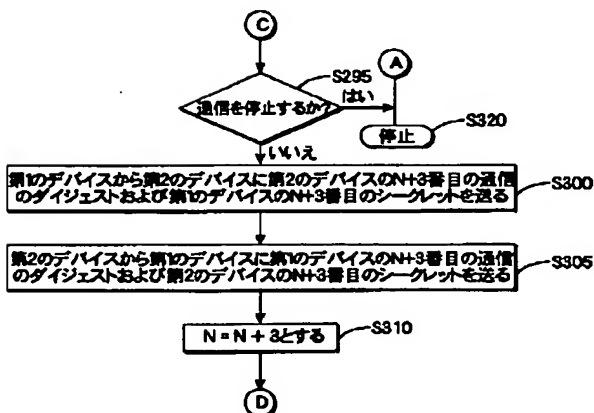
【図3】



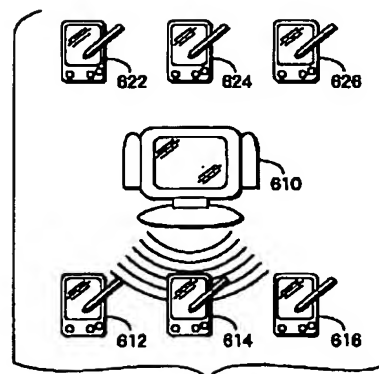
【図4】



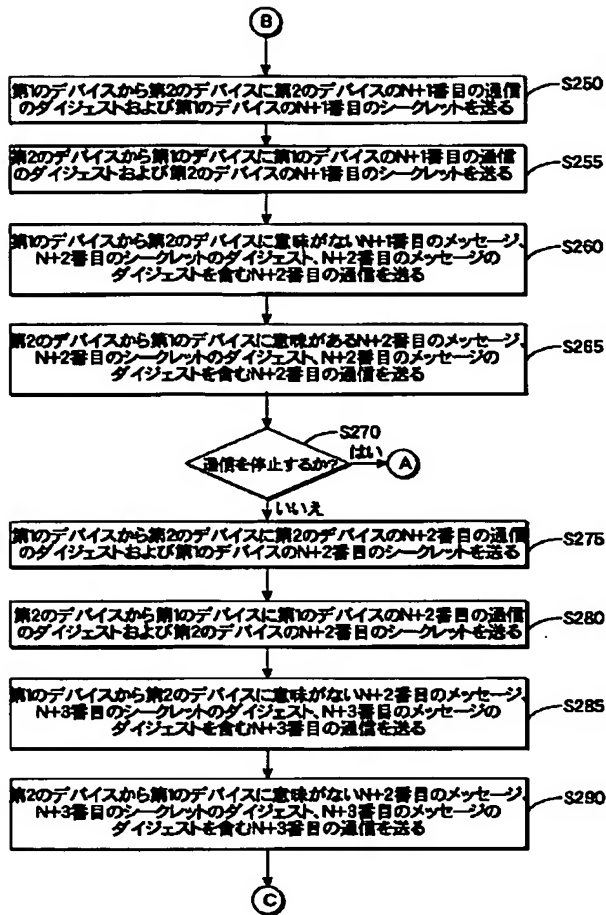
【図6】



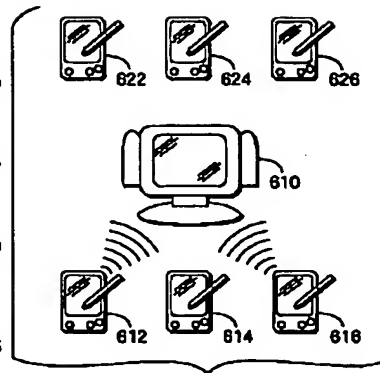
【図7】



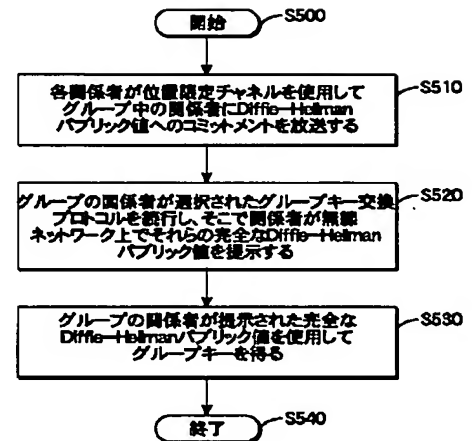
【図5】



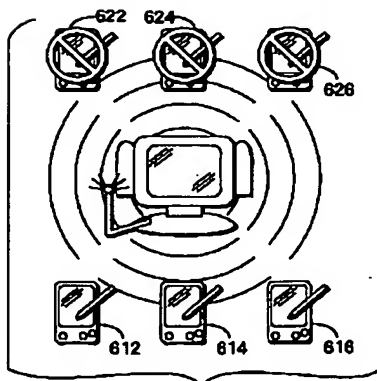
【図8】



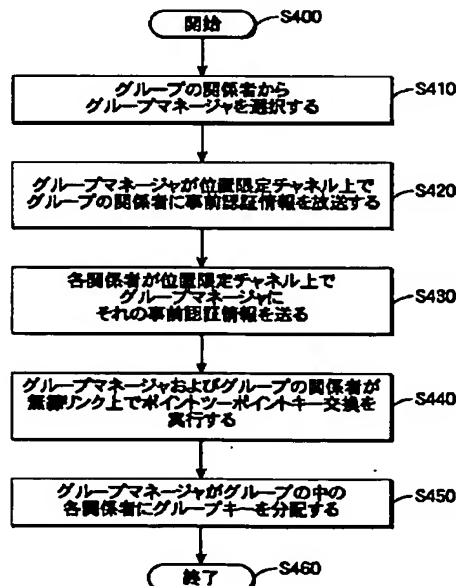
【図11】



【図9】



【図10】



フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 Q 7/38		H 0 4 L 9/00	6 0 1 C
(72) 発明者	クリスティーナ ブイ ロペス アメリカ合衆国 カリフォルニア サンフ ランシスコ ゴンザレス ドライブ 750 #12エイチ	(72) 発明者	ハオ チー ウォン アメリカ合衆国 カリフォルニア サン カルロス セダー ストリート 368
(72) 発明者	ダイアナ ケイ シュメタース アメリカ合衆国 カリフォルニア パーリ ンゲーム ラグーナ アベニュー 952	Fターム (参考)	5B085 AE04 5J104 AA01 AA07 AA16 EA04 EA19 EA21 EA24 JA21 KA02 KA05 KA06 NA02 NA12 NA24 PA01 PA07
(72) 発明者	ポール ジョセフ スチュワート アメリカ合衆国 カリフォルニア サニー ベイル ルイス ドライブ 864	5K033 AA08 CB01 CC01 DA02 DA17 DB14 DB16 EA03 5K067 AA30 DD17 DD23 EE02 EE25 GG01 GG11 HH22 HH23 HH24	